Medical Data Privacy and Ethics in the Age of Artificial Intelligence Syllabus

1. Basic Course Information

Course Name	Medical Data Privacy and Ethics in the Age of Artificial Intelligence	Course Code	BME2133
Course Level*	Graduate	Credit/Contact Hour	3.0/48
Major	Biomedical Engineering	Teaching Language	Chinese, English
Prerequisite	N/A	Prerequisite suggestion	Python Programming
School/Institute	School of Biomedical Engineering	Instructor**	Zhiyu Wan

*Notes: *Course level includes undergraduate, graduate, or undergraduate/graduate.*

**If multiple instructors are involved，please list the name of team leader.

2. Course Introduction

" Medical Data Privacy and Ethics in the Age of Artificial Intelligence " is a specialized elective course for graduate students majoring in Biomedical Engineering and a foundational public course for Master of Engineering students in Biomedical Engineering. This course focuses on issues related to medical data privacy and ethics in the age of artificial intelligence (AI), with an in-depth exploration of privacy protection technologies, ethical dilemmas, and legal regulations surrounding medical data. The curriculum covers ethical challenges and privacy protection strategies that may arise during the collection, sharing, processing, and use of medical data. Through lectures, discussions, case studies, and project-based practice, this course aims to develop students' capabilities in designing intelligent medical systems and managing biomedical data. It helps students understand how to balance privacy protection with technological innovation in AI-driven healthcare data systems, and provides a solid foundation in ethics, law, and technical practices for their future work in medical data processing.

The course comprises four fundamental modules: the first part introduces basic concepts and major challenges of data privacy and ethics in the age of artificial intelligence; the second part discusses social and legal approaches to protecting data privacy and ethics; the third part covers technical methods for privacy and ethics protection; and the fourth part applies these privacy and ethics protection methods to specific cases.

3. Learning Goal

1. Understand the core concepts, main challenges, and technical solutions related to medical data privacy and ethics in the age of artificial intelligence.

2. Explore ethical issues in medical data processing with AI, such as algorithmic bias, transparency, and informed consent.

3. Learn relevant domestic and international laws and regulations, such as HIPAA and GDPR, regarding medical data privacy protection.

4. Master common and advanced techniques for medical data privacy protection, including differential privacy, encryption methods, and de-identification techniques.

5. Develop critical thinking on data privacy and ethics in intelligent medicine and enhance practical skills for addressing privacy and ethical issues to support the design and implementation of future AI healthcare systems.

4. Instructional Pedagogy

This course is primarily lecture-based, with group discussions and literature reviews to enhance students' understanding of theory, and case studies and project-based practice to strengthen their ability to apply theory and techniques. It aims to improve students' skills in solving complex data privacy and ethical issues in real-world scenarios. A combination of lectures, in-class quizzes, reading summaries, homework assignments, case discussions, special topic seminars, and course research projects is employed, emphasizing an understanding-based, heuristic teaching approach aligned with international standards. This approach encourages students' active learning and research interest. Additionally, teaching can be supplemented with MOOCs, guest lectures, and other methods. The primary spoken language is Chinese, while written materials are primarily in English.

5. Course Content and Schedule

(You might choose one of the two course structures listed below. Please list practical training if any.)

Course Structure by Week

Week	Chapter	Teaching Contents	Contact Hours	Teaching Modes
Week 1, Wednesday Feb 19, 15:00-16:40	I. Course Introduction and Overview of Data Privacy and Ethics (a)(b)	The Role of Medical Data in the Age of AI. Concept of data privacy and its importance. Concept of ethics and morality and their importance.	2	Lectures, case discussions, and group discussions
Week 1, Friday Feb 21, 15:00-16:40	I. Course Introduction and Overview of Data Privacy and Ethics (c)	AI ethics: machine morality and ethics, automation, and employment.	2	Lectures, case discussions, and group discussions
	II. Ethical Issues in Life Sciences, Medicine, and Informatics (a)	Research ethics: ethical guidelines for human and animal experiments and scientific research. Life sciences ethics: controversies arising from reproductive technology, genetic technology, stem cell research, etc.		
Week 2, Friday Feb 28, 15:00-16:40	II. Ethical Issues in Life Sciences, Medicine, and Informatics (b)(c)	Medical ethics issues: abortion, euthanasia, public health issues, and medical ethics concerning special populations (infants, adolescents, psychiatric patients, etc.).	2	Lectures and case discussions

		Information security and privacy issues: personal data breaches, surveillance technology, facial recognition. Cybersecurity and crimes: hacking, cyberbullying.		
Week 3, Wednesday March 5, 15:00-16:40	III. Ethical Issues in Data Sharing and Medical AI (a)(b)	Importance of biomedical data sharing and privacy challenges. Data governance and data lifecycle management. Algorithmic fairness and bias issues. The importance of transparency and interpretability in medical AI.	2	Lectures and case discussions
Week 3, Friday March 7, 15:00-16:40	III. Ethical Issues in Data Sharing and Medical AI (c)	**In-class quiz 1** Digital implementation of patient informed consent.	2	Lectures and case discussions
	IV. Legal and Regulatory Frameworks (a)	The impact of international laws and regulations like HIPAA and GDPR on the impact of biomedical data.		
Week 4, Friday March 14, 15:00-16:40	IV. Legal and Regulatory Frameworks (b)(c)	China's data security law and personal information protection law. Compliance requirements for medical data sharing.	2	Lectures and case discussions
Week 5, Wednesday March 19, 15:00-16:40	V. Characteristics and Privacy Risks of Biomedical Data I (a)(b)	**In-class quiz 2.** Characteristics and privacy risks of electronic health records. Characteristics and privacy risks of natural language medical data.	2	Lectures and case discussions

		Characteristics and privacy risks of genomic data.		
Week 5, Friday March 21, 15:00-16:40	V. Characteristics and Privacy Risks of Biomedical Data I (c)	Characteristics and privacy risks of medical image data.	2	Lectures and case discussions
	VI. Characteristics and Privacy Risks of Biomedical Data II (a)	Main attack models: re-identification attacks, membership inference attacks, and reconstruction attacks.		
Week 6, Friday March 28, 15:00-16:40	VI. Characteristics and Privacy Risks of Biomedical Data II (b)(c)	Privacy Risk Assessment Methods. Case studies on breaches of different types of medical data. **Homework assignment 1.**	2	Lectures and case discussions
Week 7, Wednesday April 2, 15:00-16:40	VII. Common Privacy Protection Techniques for Medical Data I (a)(b)	Data de-identification techniques: pseudonymization, K-anonymization, etc.	2	Lectures
Week 7, Friday April 4, 15:00-16:40	VII. Common Privacy Protection Techniques for Medical Data I (c)	Game-theoretic models for optimized protection.	2	Lectures
	VIII. Common Privacy Protection Techniques for Medical Data II (a)	Basic principles and applications of differential privacy I. **Start selecting topics for the course project.**		

Week 8, Friday April 11, 15:00-16:40	VIII. Common Privacy Protection Techniques for Medical Data II (b)(c)	Basic principles and applications of differential privacy II. Access control and audit techniques. **Homework assignment 2.**	2	Lectures
Week 9, Wednesday April 16, 15:00-16:40	IX. Common Privacy Protection Techniques for Medical Data III (a)(b)	Basics of cryptography. Methods and Applications of homomorphic encryption technologies for privacy-preserving computing in medicine. Methods and Applications of secure multi-party computation technologies for privacy-preserving computing in medicine.	2	Lectures
Week 9, Friday April 18, 15:00-16:40	IX. Common Privacy Protection Techniques for Medical Data III (c)	Methods and Applications of encrypted hardware technologies for privacy-preserving computing in medicine.	2	Lectures
	X. Advances in Frontier Technologies and Future Trends in Medical Data Privacy Protection I (a)	Methods and Applications of federated learning models in privacy protection.		
Week 10, Friday	X. Advances in Frontier Technologies and	Methods and Applications of synthetic data generation techniques in privacy protection.	2	Lectures

April 25, 15:00-16:40	Future Trends in Medical Data Privacy Protection I (b)(c)	**Homework assignment 3.**		
Week 11, Wednesday April 30, 15:00-16:40	XI. Advances in Frontier Technologies and Future Trends in Medical Data Privacy Protection II (a)(b)	The potential of blockchain technology in medical data privacy.	2	Lectures
Week 11, Friday May 2, 15:00-16:40	XI. Advances in Frontier Technologies and Future Trends in Medical Data Privacy Protection II (c)	Future trends in medical data privacy research.	2	Lectures
	XII. Privacy and Ethical Issues in Cutting-Edge AI Technologies for Healthcare I (a)	Introduction to large language models. Applications of large language models in medicine.		
Week 12, Friday May 9, 15:00-16:40	XII. Privacy and Ethical Issues in Cutting-Edge AI Technologies for Healthcare I (b)(c)	Privacy risk issues of large language models. **Presentations of team project proposals.**	2	Lectures

Week 13, Wednesday May 14, 15:00-16:40	XIII. Privacy and Ethical Issues in Cutting-Edge AI Technologies for Healthcare II (a)(b)	Fairness issues of large language models. Other ethical issues of large language models.	2	Lectures and case discussions
Week 13, Friday May 16, 15:00-16:40	XIII. Privacy and Ethical Issues in Cutting-Edge AI Technologies for Healthcare II (c)	Solutions to ethical issues of large language models and future directions.	2	Lectures and case discussions
	XIV. Privacy and Ethical Issues in Cutting-Edge AI Technologies for Healthcare III (a)	Introduction to generative artificial intelligence. Applications of generative artificial intelligence in medicine.		
Week 14, Friday May 23, 15:00-16:40	XIV. Privacy and Ethical Issues in Cutting-Edge AI Technologies for Healthcare III (b)(c)	Potential privacy risks and ethical issues of medical diagnosis and treatment models based on generative artificial intelligence. Discussion and outlook on potential ethical and privacy issues arising from the development of artificial general intelligence.	2	Lectures, case discussions, and group discussions
Week 15, Wednesday May 28, 15:00-16:40	XV. Special Topic Lectures (a)(b)	Two experts will be invited to present cases of medical data attacks or protection in specific application scenarios (different modalities, different diseases).	2	Lectures

Week 15, Friday May 30, 15:00-16:40	XV. Special Topic Lectures (c)	One expert will be invited to present cases of medical data attacks or protection in specific application scenarios (different modalities, different diseases).	1	Lectures
	XVI. Course Project Presentation (a)	Group presentations and feedback.	1	Group presentations
Week 16, Friday June 6, 15:00-16:40	XVI. Course Project Presentation (b)(c)	Group presentations and feedback.	2	Group presentations

Course Structure by Chapter

Chapter	Teaching Contents	Week	Contact Hours	Teaching Modes
/	/	/	/	/

6.Grading Policy

This course does not have a final exam; instead, it primarily assesses students' grasp of the content through a team project-based approach. Each team, composed of 1-2 students, will choose a project from a list of topics provided by the course instructor. They will conduct a literature review, investigate existing solutions, identify and summarize remaining challenges, and propose their own solutions. The teams will then seek relevant datasets to conduct experimental validation. Each team is required to have data-based experimental results, deliver an oral presentation, and submit a project report in the form of a paper written in English. With prior notice and approval from the course instructor, students may also select a topic outside the provided list for topics. The schedule for the course project is as follows:

Week	Course Project Planning
8	Announce course project topics, and students begin forming teams.
9	Students complete team formation and begin selecting course project topics.
10	Each team **completes project topic selection** and begins preparing a preliminary project proposal.
12	Each team **presents a project proposal** for 5 minutes in class and **submits a 4-page preliminary project proposal**.
13	The instructor and teaching assistants conduct a mid-term evaluation of each team's preliminary project proposal and provide feedback and guidance to each team. Students then prepare their final course project based on the feedback.
16	Each team gives an **in-class oral presentation** of approximately 10 minutes (timing adjusted based on the total number of teams, with the presentation order not disclosed in advance. Note: all teams are required to submit PPT before the first presentation). The instructor, invited experts, teaching assistants, and all students will provide fair and impartial ranking and scoring for each team's presentation.
17	Students **submit the final course project report** (an updated 10-page project report. Note: co-authors are listed without ranking, but each co-author's responsibilities and contributions must be specified in the report).
18	The instructor and teaching assistants conduct a final evaluation of the course project reports.

The grading breakdown for the course project is as follows: mid-term evaluation (20%) + oral presentation performance (40%) + project report (40%). The grading for the preliminary project proposal and the project report is assisted by the teaching assistant and is finally determined by the instructor. The score for the oral presentation performance is obtained through a weighted average: instructor (50%), invited experts (20%), teaching assistants (10%), and all students (20%). The score from all students is calculated as the average of scores given by students, excluding team members of the presenting group, and with the highest and lowest scores removed.

The overall assessment breakdown is shown in the table below:

1	Course Project	50%
2	Homework Assignments	30%
3	Reading Summaries	10%
4	In-class quizzes	5%
5	Attendances and Classroom Performance	5%
	Total	100%

Tests and submitted assignments are primarily in English. There are a total of three homework assignments, which include Q&A, calculation, and programming tasks, etc. Collaboration is not allowed. Each homework assignment carries equal weight. From week 2 to week 13, there are three assigned (one required and two optional) pre-class readings per week. Students are required to write summaries of the readings, which contribute 10% to the overall grade as an average score. In-class quizzes (closed-book) are given twice, in weeks 3 and 5, covering material from weeks 1-2 and 3-4, respectively. Both quizzes carry equal weight. Grades and comments for homework, pre-class reading summaries, and quizzes are provided within two weeks. Attendance is randomly checked by selecting students to answer questions in class; if a student is absent without prior notice, 1% is deducted from their overall grade, up to a maximum of 5%. Students who have excused absences may have no attendance points deducted as appropriate. The final overall score will be converted from a percentage to a letter grade. The conversion relationship is shown in the table below:

Grade	A+	A	A-	B+	B	B-	C+	C	C-	F	EXC	P	NP	N
Grade Point	4.0	4.0	3.7	3.3	3.0	2.7	2.3	2	1.7	0	N/A	N/A	N/A	N/A
Reference Percentage-to-Grade Conversion Scale	95-100	90-94	85-89	80-84	75-79	70-74	67-69	63-66	60-62	0-59	As per the course syllabus	>=60	<60	No grade record

It is recommended that if the class size exceeds 30 students, no more than 40% should receive an A- or above, and the failure rate should not exceed 10%.

7. Textbook & Recommended Reading

(1) Textbook

Recommended Textbook 1：

*Book Name: Medical Data Privacy Handbook	*Author: Aris Gkoulalas-Divanis, Grigorios Loukides	Translator:	*ISBN: 9783319236322
*Publisher: Springer	*Publication Month: 2015.12	*Version: 1	

Recommended Textbook 1：

*Book Name: 工程伦理	*Authors: 李正风、王前、丛杭青	Translator:	*ISBN: 9787302524670
* Publisher: 清华大学出版社	*Publication Month: 2019.06	* Version: 2	

(2) Recommended Reading

Recommended Reading 1:

Book Name: Ethics of Medical AI	Author: Giovanni Rubeis	Translator:	ISBN: 9783031557439
Publisher: Springer	Publication Month: 2024.03	Version: v2024	

Recommended Reading 2:

Book Name: Guide to the De-Identification of Personal Health Information	Author: Khaled El Emam	Translator:	ISBN: 9780429100659
Publisher: Auerbach Publications	Publication Month: 2013.05	Version: 1	

Recommended Reading 3:

Book Name: Ethics and Data Science	Authors: Mike Loukides, Hilary Mason, DJ Patil	Translator:	ISBN: 9781492043881
Publisher: O'Reilly Media, Inc.	Publication Month: 2018.07	Version: 1	

Recommended Reading 4:

Book Name: Responsible Genomic Data Sharing: Challenges and Approaches	Authors: Xiaoqian Jiang, Haixu Tang	Translator:	ISBN: 9780128163399
Publisher: Academic Press	Publication Month: 2020.03	Version: 1	

8. Academic Integrity

This course highly values academic integrity. Behaviors such as plagiarism and cheating are strictly prohibited. Please list more if you have more specific requirements.

9. Other Information (Optional)